AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application. Please cancel claim 13. Please amend claims 1-12, 14-18, and 20-23, and add new claim 24 as follows.

Listing of Claims

1. (Currently Amended) A digital private key protection device, comprising:

a digital ~~private~~ key storage ~~means~~ containing a user's digital private key;

a cryptographic engine for processing digital data and one or more digital keys;

a communications port for receiving digital data including a document to be signed from an external device, and for transmitting data ~~to said~~ external of said digital private key protection device;

a trusted display ~~means~~ for displaying said received digital data including a document;

a user operable input ~~means~~ connected to said cryptographic engine to indicate when operated by said user their approval of said displayed received digital data including a document; wherein

said cryptographic engine is trusted to only apply said user's digital private key to sign said received digital data only if said user operable input ~~means~~ is operated and communicate said signed data including a document external of said digital private key protection device.

2. (Currently Amended) A digital private key protection device according to claim 1, wherein said digital ~~private~~ key storage ~~means~~ also contains a trusted public key and a plurality of user's public keys signed ~~by said digital private~~ so as to be verifiable by the trusted public key; and said cryptographic engine validates signature of said user's public key with said trusted public key to determine the veracity of a said user's public key and then processes ~~decrypts~~ said received digital data using said verified predetermined user's public key and causes said trusted display to indicate whether said user's private key was used to sign said received digital data.

3. (Currently Amended) A digital private key protection device according to claim 1, wherein said received digital data includes a digital certificate. ~~for said digital data created~~

~~using a user's private key or a digital private key or a secret key of a digital private key protection device.~~

4. (Currently Amended) A digital private key protection device according to claim 1 further comprising an audit means wherein signed data is not transmitted external of said digital private key protection device until ~~a said cryptographic engine process is audited by~~ said audit means audits the signing performed by said cryptographic engine.

5. (Currently Amended) A digital private key protection device according to claim 2 further comprising an audit means wherein signed received digital data is not displayed by said trusted display until ~~a said cryptographic engine process is audited by~~ said audit means audits the signing performed by said cryptographic engine.

6. (Currently Amended) A digital private key protection device according to claim 1 wherein said digital ~~private~~ key ~~protection device~~ storage further ~~comprises a~~ includes said digital private key protection device's ~~device~~ private key ~~storage means~~ wherein digital data signed by said digital private key protection device after operation of said user operable input ~~means~~ is further signed by said private key of said digital private key protection device.

7. (Currently Amended) A digital private key protection device according to claim ~~1~~ 6 wherein said digital ~~private~~ key storage ~~means contains a predetermined~~ also includes said digital private key protection device's public key; such that when said communications port receives signed digital data from an external device which may or may not have been signed by ~~a~~ said ~~predetermined~~ digital private key protection device's private key;

said cryptographic engine decrypts said received data using said ~~predetermined~~ digital private key protection device's public key to verify whether said digital private key protection device's predetermined digital private key was used to encrypt said received digital data.

8. (Currently Amended) A digital private key protection device according to claim 7 wherein said trusted display means indicates whether said digital private key protection device's private key was used to encrypt said received digital data.

9. (Currently Amended) A digital private key protection device according to claim 1 ~~further comprising a public~~ the digital key storage ~~means containing~~ includes a plurality of user's public keys; and

said received digital data contains information that predetermines which user's public key is used to ~~sign~~ encrypt said received digital data that is transmitted external of said digital private key protection device to a predetermined user.

10. (Currently Amended) A digital private key protection device according to claim 1 wherein said cryptographic engine is trusted to decrypt received digital data using said user's digital private key and passing decrypted digital data to said trusted display ~~means~~ for display of said received digital data.

11. (Currently Amended) A digital private key protection device according to claim 10 wherein decrypted ~~information~~ received digital data is not released external to said device unless said user operable input ~~means~~ is operated.

12. (Currently Amended) A digital private key protection device according to claim 10 wherein said communications port ~~can not~~ cannot transmit said decrypted digital data external of said digital private key protection device.

13. (Canceled)

14. (Currently Amended) A digital private key protection device according to claim 1 wherein said digital ~~private~~ key storage ~~means~~ also contains a digital shared secret symmetric key wherein said cryptographic engine ~~is trusted to~~ only ~~apply~~ applies said digital shared secret symmetric key to encrypt signed received digital data only if said user operable input means is operated and ~~also trusted~~ to communicate said encrypted signed received digital data external of said digital private key protection device.

15. (Currently Amended) A digital private key protection device according to claim 1, wherein said received digital data contains an instruction which determines how said

~~encryption~~ cryptographic engine should ~~encrypt or decrypt respectively~~process the received digital data.

16. (Currently Amended) A digital private key protection device according to claim 1, wherein said received digital data contains an instruction which determines which protocol is used by said digital private key protection device to communicate encrypted or signed received digital data external of said digital private key protection device.

17. (Currently Amended) A digital private key protection device according to claim 1, wherein said trusted display ~~means~~ is external to said digital private key protection device and controlled by said digital private key protection device for displaying data transmitted from said communications port in a trusted manner.

18. (Currently Amended) A digital private key protection device according to claim 1, wherein said user operable input ~~means~~ is external to said digital private key protection device and controlled by said digital private key protection device to be actuated by said user in a predetermined manner.

19. (Previously Presented) A digital private key protection device according to claim 1, further comprising identification and authentication means actuated by said user in a predetermined manner.

20. (Currently Amended) A digital private key protection device according to claim ~~18~~ 1 further comprising an audit means which audits ~~said~~ the actuation of said user operable input ~~means~~.

21. (Currently Amended) A digital private key protection device according to claim 1, wherein ~~said~~ the digital ~~private~~ key storage ~~means~~ is removable from said digital private key protection device.

22. (Currently Amended) A digital private key protection device according to claim ~~16~~, wherein a cryptographic request is received from ~~said~~ an external device according to a

predetermined application programming interface, such that the request is performed by said digital private key protection device using the user's private or other keys as identified by the request, but excluding ~~the~~ any private keys associated with the digital private key protection device with the result being transmitted to said external device or a predetermined destination included in said request or otherwise predetermined.

23. (Currently Amended) A digital private key protection device according to claim 22 wherein said ~~device~~ trusted display displays a description of said cryptographic request to the user and, only if the user operates said user operable input ~~means~~, does said digital private key protection device carry out said cryptographic request.

24. (New) A digital private key protection device according to claim 1, wherein the digital key storage is adapted to allow removal of the user's digital keys from the digital private key protection device.